When we get a javacript-heavy application we want to do a few different things.

- Increase the attack-surface - Find URL:s or domains
- Sensitive information - API-keys, passwords
- Potentially dangerous areas of code - eval, setDangerousInnerHTML
- Component with known vulnerabilities

Luckily this can be done using static analysis.

Step 1. Identify all javascript files

First navigate through the entire application manually while using burp. When you are done go to:

```
Site map - select target - engagement tools - find scripts
```

Step 2. Find URL:s

```
python linkfinder.py -i https://example.com -d -o cli
```

Step 3. Find sensitive information

TruffleHog can find sensitive information.

```
truffleHog
```